

ACKNOWLEDGEMENT

First of all I would like to give my heartfelt gratitude to God for enabling me to express my inspiration in this piece of paper. Next, I express my sincere gratitude to Mr. Rajesh and Mrs.A.Rajini for their guidance and utmost advice to complete this seminar work successfully. Beyond this, I like to thank them for awakening my perception to focus on building my technical skills to be outstanding in this competitive and dynamic digital world. Their sincere brotherly advice will remain my motivation to excel in my proceeding academic career.

ABSTRACT

Security is always a burning issue in wireless and mobile communication networks. There has been a serious problem with security issues since the inception of Wireless communication technology. The primary challenge is the way to avoid malicious threats from interfering in a certain network. To solve this challenge in generation of mobile networks different key security management schemes has been designed to nullify any vulnerable entities and as a result detach tainted network devices. Here network operators will verify for themselves associate in nursing best interval for updates that minimizes the communication load they impose, whereas protective of user mobility. The comparison of security issues handling mechanism of all generations of wireless and mobile communications is thoroughly reflected upon in this seminar paper.

TABLE OF CONTENTS

Contents

ACKNOWLEDGEMENT	i
ABSTRACT	i
TABLE OF CONTENTS	iii
LIST OF FIGURES	v
CHAPTER ONE	1
OVERVIEW OF WIRELESS AND MOBILE NETWORK SECURITY	1
1.1 Introduction:.....	1
1.2 Second generation to fourth generation (2G-4G) security rationale	5
CHAPTER 2	7
SECURITY IN FIRST GENERATION (1G) WIRELESS MOBILE TECHNOLOGY	7
2.1. Features of 1G:.....	7
2.2. Security Threats:	7
CHAPTER 3	8
SECURITY IN SECOND GENERATION (2G) WIRELESS MOBILE TECHNOLOGY	8
3.1 Features of 2G	8
3.2. Security issues in 2G wireless mobile networks	11
CHAPTER 4	13
SECURITY IN THIRD GENERATION WIRELESS MOBILE TECHNOLOGY (3G)	13
4.1 Features of 3G.....	13
4.2 Types of Threats for 3G	13
4.3 Security enhancement in 3G wireless and mobile technology.....	14
CHAPTER 5	22
SECURITY IN FOURTH GENERATION (4G) WIRELESS AND MOBILE TECHNOLOGY ...	22
5.1 Features of 4G	22
5.2 Security Threats of 4G	23
5.3. 4G Wireless and mobile technology Security Enhancement Issues	24
CHAPTER 6	27
SECURITY IN FIFTH GENERATION (5G) WIRELESS AND MOBILE TECHNOLOGY	27
6.1 Features of 5G.....	27
6.2 Security characteristics of 5G	28
6.3 Core 5G Security Topics.....	31

6.4 Security infrastructure of 5G.....	35
CHAPTER 7	37
CONCLUSION.....	37
REFERENCES	38

LIST OF FIGURES

<i>Figure 1 Simplified GSM Network Architecture Diagram.</i>	<i>11</i>
<i>Figure 2 WAP Programming model using a wireless gateway (or proxy).</i>	<i>15</i>
<i>Figure 3: WAP programming model without gateway.</i>	<i>16</i>
<i>Figure 4: WAP architecture and its relationship to the OSI model.</i>	<i>17</i>
<i>Figure 5 Seamless connections of networks in 4G</i>	<i>23</i>
<i>Figure 6 The eight Security dimensions of 4G.</i>	<i>25</i>
<i>Figure 7 Architecture of proposed 5G technology</i>	<i>27</i>
<i>Figure 8 The defining characteristics of 5G security</i>	<i>30</i>
<i>Figure 9 High level 5G security Principles</i>	<i>33</i>
<i>Figure 10 Link security level between user, network and service giver.</i>	<i>36</i>

CHAPTER ONE

OVERVIEW OF WIRELESS AND MOBILE NETWORK SECURITY

“The precondition to freedom is Security”

Rand beers

1.1 Introduction:

Wireless and mobile networks have undergone a tremendous evolution since their start. This was mainly motivated by the need for connectivity everywhere, as exemplified by the philosophy of “always on” access. Mobile telephony was the first need felt by users, followed by the need for mobile Internet applications. Mobile telecommunications networks were the first concretization of mobile telephony, followed by a set of wireless technologies with or without embedded mobility and with or without infrastructure. Obviously, this large deployment of services over mobile and wireless networks is not easy from a network security point of view.

Mobile devices face an array of threats that take advantage of numerous vulnerabilities commonly found in such devices. These vulnerabilities can be the result of inadequate technical controls, but they can also result from the poor security practices of consumers. Companies and relevant agencies have taken steps to improve the security of mobile devices, including making certain controls available for consumers to use if they wish and promulgating information about recommended mobile security practices. However, security controls are not always consistently implemented on mobile devices, and it is unclear whether consumers are aware of the importance of enabling security controls on their devices and adopting recommended practices.

A list of mobile vulnerabilities that is common to all mobile platforms are:-

- Mobile devices often do not have passwords enabled. Mobile devices often lack passwords to authenticate users and control access to data stored on the devices. Many devices have the technical capability to support passwords, personal identification numbers (PIN), or pattern screen locks for authentication. Some mobile devices also include a biometric reader to scan a fingerprint for authentication. However, anecdotal information indicates that consumers seldom employ these mechanisms. Additionally, if users do use a password or PIN they often choose passwords or PINs that can be easily determined or bypassed, such as 1234 or 0000. Without passwords or PINs to lock the device, there is increased risk that stolen or lost phones' information could be accessed by unauthorized users who could view sensitive information and misuse mobile devices.
- Two-factor authentication is not always used when conducting sensitive transactions on mobile devices. According to studies, consumers generally use static passwords instead of two-factor authentication when conducting online sensitive transactions

while using mobile devices. Using static passwords for authentication has security drawbacks: passwords can be guessed, forgotten, written down and stolen, or eavesdropped. Two-factor authentication generally provides a higher level of security than traditional passwords and PINs, and this higher level may be important for sensitive transactions. Two-factor refers to an authentication system in which users are required to authenticate using at least two different "factors" — something you know, something you have, or something you are — before being granted access. Mobile devices can be used as a second factor in some two-factor authentication schemes. The mobile device can generate pass codes, or the codes can be sent via a text message to the phone. Without two-factor authentication, increased risk exists that unauthorized users could gain access to sensitive information and misuse mobile devices.

- Wireless transmissions are not always encrypted. Information such as e-mails sent by a mobile device is usually not encrypted while in transit. In addition, many applications do not encrypt the data they transmit and receive over the network, making it easy for the data to be intercepted. For example, if an application is transmitting data over an unencrypted WiFi network using http (rather than secure http), the data can be easily intercepted. When a wireless transmission is not encrypted, data can be easily intercepted.
- Mobile devices may contain malware. Consumers may download applications that contain malware. Consumers download malware unknowingly because it can be disguised as a game, security patch, utility, or other useful application. It is difficult for users to tell the difference between a legitimate application and one containing malware. For example, an application could be repackaged with malware and a consumer could inadvertently download it onto a mobile device. The data can be easily intercepted. When a wireless transmission is not encrypted, data can be easily intercepted by eavesdroppers, who may gain unauthorized access to sensitive information.
- Mobile devices often do not use security software. Many mobile devices do not come preinstalled with security software to protect against malicious applications, spyware, and malware-based attacks. Further, users do not always install security software, in part because mobile devices often do not come preloaded with such software. While such software may slow operations and affect battery life on some mobile devices, without it, the risk may be increased that an attacker could successfully distribute malware such as viruses, Trojans, spyware, and spam to lure users into revealing passwords or other confidential information.
- Operating systems may be out-of-date. Security patches or fixes for mobile devices' operating systems are not always installed on mobile devices in a timely manner. It can take weeks to months before security updates are provided to consumers' devices. Depending on the nature of the vulnerability, the patching process may be complex and involve many parties. For example, Google develops updates to fix security vulnerabilities in the Android OS, but it is up to device manufacturers to produce a device-specific update incorporating the vulnerability fix, which can take time if there are proprietary modifications to the device's software. Once a manufacturer produces

an update, it is up to each carrier to test it and transmit the updates to consumers' devices. However, carriers can be delayed in providing the updates because they need time to test whether they interfere with other aspects of the device or the software installed on it.

- In addition, mobile devices that are older than two years may not receive security updates because manufacturers may no longer support these devices. Many manufacturers stop supporting smartphones as soon as 12 to 18 months after their release. Such devices may face increased risk if manufacturers do not develop patches for newly discovered vulnerabilities.
- Software on mobile devices may be out-of-date. Security patches for third-party applications are not always developed and released in a timely manner. In addition, mobile third-party applications, including web browsers, do not always notify consumers when updates are available. Unlike traditional web browsers, mobile browsers rarely get updates. Using out-dated software increases the risk that an attacker may exploit vulnerabilities associated with these devices.
- Mobile devices often do not limit Internet connections. Many mobile devices do not have firewalls to limit connections. When the device is connected to a wide area network it uses communications ports to connect with other devices and the Internet. A hacker could access the mobile device through a port that is not secured. A firewall secures these ports and allows the user to choose what connections he wants to allow into the mobile device. Without a firewall, the mobile device may be open to intrusion through an unsecured communications port, and an intruder may be able to obtain sensitive information on the device and misuse it.
- Mobile devices may have unauthorized modifications. The process of modifying a mobile device to remove its limitations so consumers can add features (known as "jail-breaking" or "rooting") changes how security for the device is managed and could increase security risks. Jail-breaking allows users to gain access to the operating system of a device so as to permit the installation of unauthorized software functions and applications and/or to not be tied to a particular wireless carrier. While some users may jailbreak or root their mobile devices specifically to install security enhancements such as firewalls, others may simply be looking for a less expensive or easier way to install desirable applications. In the latter case, users face increased security risks, because they are bypassing the application vetting process established by the manufacturer and thus have less protection against inadvertently installing malware. Further, jail-broken devices may not receive notifications of security updates from the manufacturer and may require extra effort from the user to maintain up-to-date software.
- Communication channels may be poorly secured. Having communication channels, such as Bluetooth communications, "open" or in "discovery" mode (which allows the device to be seen by other Bluetooth-enabled devices so that connections can be made) could allow an attacker to install malware through that connection, or surreptitiously activate a microphone or camera to eavesdrop on the user. In addition, using unsecured public wireless Internet networks or WiFi spots could allow an attacker to connect to the device and view sensitive information.

- Connecting to an unsecured WiFi network could let attacker access personal information from a device, putting users at risk for data and identity theft. One type of attack that exploits the WiFi network is known as man-in-the-middle, where an attacker inserts himself in the middle of the communication stream and steals information.

So what can be done to secure mobile devices? Generally, The US government authentication (GAO) offers a number of ideas including:

- ❖ Enable user authentication: Devices can be configured to require passwords or PINs to gain access. In addition, the password field can be masked to prevent it from being observed, and the devices can activate idle-time screen locking to prevent unauthorized access.
- ❖ Enable two-factor authentication for sensitive transactions: Two-factor authentication can be used when conducting sensitive transactions on mobile devices. Two-factor authentication provides a higher level of security than traditional passwords. Two-factor refers to an authentication system in which users are required to authenticate using at least two different "factors" — something you know, something you have, or something you are — before being granted access. Mobile devices themselves can be used as a second factor in some two-factor authentication schemes used for remote access. The mobile device can generate pass codes, or the codes can be sent via a text message to the phone. Two-factor authentication may be important when sensitive transactions occur, such as for mobile banking or conducting financial transactions.
- ❖ Verify the authenticity of downloaded applications: Procedures can be implemented for assessing the digital signatures of downloaded applications to ensure that they have not been tampered with.
- ❖ Install antimalware capability: Antimalware protection can be installed to protect against malicious applications, viruses, spyware, infected secure digital cards, and malware-based attacks. In addition, such capabilities can protect against unwanted (spam) voice messages, text messages, and e-mail attachments.
- ❖ Install a firewall: A personal firewall can protect against unauthorized connections by intercepting both incoming and outgoing connection attempts and blocking or permitting them based on a list of rules.
- ❖ Install security updates: Software updates can be automatically transferred from the manufacturer or carrier directly to a mobile device. Procedures can be implemented to ensure these updates are transmitted promptly.
- ❖ Install antimalware capability: Antimalware protection can be installed to protect against malicious applications, viruses, spyware, infected secure digital cards and malware-based attacks. In addition, such capabilities can protect against unwanted (spam) voice messages, text messages, and e-mail attachments
- ❖ Install a firewall: A personal firewall can protect against unauthorized connections by intercepting both incoming and outgoing connection attempts and blocking or permitting them based on a list of rules.

- ❖ Install security updates: Software updates can be automatically transferred from the manufacturer or carrier directly to a mobile device. Procedures can be implemented to ensure these updates are transmitted promptly.
- ❖ Remotely disable lost or stolen devices: Remote disabling is a feature for lost or stolen devices that either locks the device or completely erases its contents remotely. Locked devices can be unlocked subsequently by the user if they are recovered.
- ❖ Enable encryption for data stored on device or memory card: File encryption protects sensitive data stored on mobile devices and memory cards. Devices can have built-in encryption capabilities or use commercially available encryption tools.
- ❖ Enable whitelisting: Whitelisting is a software control that permits only known safe applications to execute commands.
- ❖ Establish a mobile device security policy: Security policies define the rules, principles, and practices that determine how an organization treats mobile devices, whether they are issued by the organization or owned by individuals. Policies should cover areas such as roles and responsibilities, infrastructure security, device security, and security assessments. By establishing policies that address these areas, agencies can create a framework for applying practices, tools, and training to help support the security of wireless networks.
- ❖ Provide mobile device security training: Training employees in an organization's mobile security policies can help to ensure that mobile devices are configured, operated, and used in a secure and appropriate manner.
- ❖ Establish a deployment plan: Following a well-designed deployment plan helps to ensure that security objectives are met.
- ❖ Perform risk assessments: Risk analysis identifies vulnerabilities and threats, enumerates potential attacks, assesses their likelihood of success, and estimates the potential damage from successful attacks on mobile devices.
- ❖ Perform configuration control and management: Configuration management ensures that mobile devices are protected against the introduction of improper modifications before, during, and after deployment.

1.2 Second generation to fourth generation (2G-4G) security rationale

Some 25 years ago, when GSM systems were developed and standardized, security functions were introduced partly because of shortcomings discovered in previous analog systems, but also because of emerging threats. First of all, encryption of the radio interface was introduced. With earlier systems, use of simple radio receivers enabled eavesdropping on conversations through mobile communication. However, at the time, export and public use of encryption was a contentious issue, which resulted in a design of only moderate strength. Nevertheless, it was regarded as strong enough for the estimated economic lifetime of GSM at that time (roughly 10 years). Secondly, risk of fraud – such as making calls charged to other subscribers – was considered a major problem. This led to the introduction of a tamper-resistant SIM card, adding strong authentication of the subscriber and, consequently, a strong binding to robust

charging. Finally, subscriber privacy entered the scene, and a mechanism with randomly assigned temporary identifiers was introduced to make it harder to track or identify subscribers.

Moving to 3G, further security improvements were made. Examples include mutual authentication to mitigate threats of rogue radio base stations, and moving the encryption deeper into the network and making it state-of-the-art in terms of strength. When the 4G LTE standard was set, the main additional security measures were a consequence of returning the user data encryption down to the base station. Specifically, more elaborate key management was introduced to protect against potential physical break-ins to radio base stations. Overall, the security offered by LTE is very similar to the strong protection of 3G.

Reflecting on the rationale behind 2G-4G security, it can be said that security was introduced to protect a basic connectivity service (voice and later packet data) in order to earn users' trust in terms of privacy, and to safeguard the ecosystem in terms of correct charging. Indeed, it must be acknowledged that this has worked extremely well. Although some attacks on GSM security have become possible over the past 10 years, this was beyond the economic lifetime for which GSM was originally designed. GSM security goals were therefore met and exceeded. Furthermore, all generations of mobile networks offer completely zero-config security from the user's point of view, thanks to automatic provisioning through SIM and universal SIM (USIM) cards. However, 5G will drive additional requirements regarding security.

CHAPTER 2

SECURITY IN FIRST GENERATION (1G) WIRELESS MOBILE TECHNOLOGY

2.1. Features of 1G:

First Generation was developed in 1979 in Japan and then at various places. It has first operated on 800MHZ_AMPS which is voice only analogue network. 1G uses frequency division multiple access technique where each channel utilizes 30KHZ/user at a time. A terminal can stay connected up to 40km from cell Tower depending on terrain. The data rate of 1G was from 2.4 Kbps to 14.4 kbps.

Use of Analog signals for data (in this case voice) transmission led to many problems those are:

1. Analog Signals does not allow advance encryption methods hence there is no security of data i.e. anybody could listen to the conversation easily by simple techniques. The user identification number could be stolen easily and which could be used to make any call and the user whose identification number was stolen had to pay the call charges.
2. Analog signals can easily be affected by interference and the call quality decreases.

2.2. Security Threats:

Uses a simple 32-bit Electronic Serial Number (ESN) to confirm whether the terminal is allowed to access the service. But soon, devices appeared that could read these ESN's from the air, & access a user's account for a short time. Anyone with a radio scanner capable of transmitting or receiving on the 800MHz band could interfere on your call. Being analog, the 800MHz band **was also susceptible** to background **noise** caused by nearby electronic devices. So, 1G Analog network became prone to security problem & network congestion arising from increasing user number. This challenge was the **major motivation** behind evolution of 2G digital network.

CHAPTER 3

SECURITY IN SECOND GENERATION (2G) WIRELESS MOBILE TECHNOLOGY

3.1 Features of 2G

Digitally encrypted network developed first in 1991 Finland. With features: text messaging, multimedia messaging, internet access. And also introduced us to the SIM card which is holding IMSI (of 15 digits usually). Used **900MHz spectrum** and later introduced on the **1800MHz band**. Used **TDMA /TDD**, One-way authentication. Use Circuit switching & Data rate: 14.4 Kbps.

The GSM network architecture as defined in the GSM specifications can be grouped into four main areas as shown on Figure 2.1

- Mobile station (MS)
- Base-Station Subsystem (BSS)
- Network and Switching Subsystem (NSS)
- Operation and Support Subsystem (OSS)

Mobile station

Mobile stations (MS), mobile equipment (ME) or as they are most widely known, cell or mobile phones are the section of a GSM cellular network that the user sees and operates. In recent years their size has fallen dramatically while the level of functionality has greatly increased. A further advantage is that the time between charges has significantly increased.

There are a number of elements to the cell phone, although the two main elements are the main hardware and the SIM.

The hardware itself contains the main elements of the mobile phone including the display, case, battery, and the electronics used to generate the signal, and process the data receiver and to be transmitted. It also contains a number known as the International Mobile Equipment Identity (IMEI). This is installed in the phone at manufacture and "cannot" be changed. It is accessed by the network during registration to check whether the equipment has been reported as stolen.

The SIM or Subscriber Identity Module contains the information that provides the identity of the user to the network. It contains a variety of information including a number known as the International Mobile Subscriber Identity (IMSI).

Base Station Subsystem (BSS)

The Base Station Subsystem (BSS) section of the GSM network architecture that is fundamentally associated with communicating with the mobiles on the network. It consists of two elements:

- **Base Transceiver Station (BTS):** The BTS used in a GSM network comprises the radio transmitter receivers, and their associated antennas that transmit and receive to directly communicate with the mobiles. The BTS is the defining element for each cell. The BTS communicates with the mobiles and the interface between the two is known as the Um interface with its associated protocols.
- **Base Station Controller (BSC):** The BSC forms the next stage back into the GSM network. It controls a group of BTSs, and is often co-located with one of the BTSs in its group. It manages the radio resources and controls items such as handover within the group of BTSs, allocates channels and the like. It communicates with the BTSs over what is termed the Abis interface.

Network Switching Subsystem (NSS)

The GSM system architecture contains a variety of different elements and is often termed the core network. It provides the main control and interfacing for the whole mobile network. The major elements within the core network include:

- **Mobile Services Switching Centre (MSC):** The main element within the core network area of the overall GSM network architecture is the Mobile switching Services Centre (MSC). The MSC acts like a normal switching node within a PSTN or ISDN, but also provides additional functionality to enable the requirements of a mobile user to be supported. These include registration, authentication, call location, inter-MSC handovers and call routing to a mobile subscriber. It also provides an interface to the PSTN so that calls can be routed from the mobile network to a phone connected to a landline. Interfaces to other MSCs are provided to enable calls to be made to mobiles on different networks.
- **Home Location Register (HLR):** This database contains all the administrative information about each subscriber along with their last known location. In this way, the GSM network is able to route calls to the relevant base station for the MS. When a user switches on their phone, the phone registers with the network and from this it is possible to determine which BTS it communicates with so that incoming calls can be routed appropriately. Even when the phone is not active (but switched on) it re-registers periodically to ensure that the network (HLR) is aware of its latest position. There is one HLR per network, although it may be distributed across various sub-centres to for operational reasons.
- **Visitor Location Register (VLR):** This contains selected information from the HLR that enables the selected services for the individual subscriber to be provided. The VLR can be implemented as a separate entity, but it is commonly realised as an integral part of the MSC, rather than a separate entity. In this way access is made faster and more convenient.
- **Equipment Identity Register (EIR):** The EIR is the entity that decides whether given mobile equipment may be allowed onto the network. Each mobile equipment has a

number known as the International Mobile Equipment Identity. This number, as mentioned above, is installed in the equipment and is checked by the network during registration. Dependent upon the information held in the EIR, the mobile may be allocated one of three states - allowed onto the network, barred access, or monitored in case its problems.

- ***Authentication Centre (AuC):*** The AuC is a protected database that contains the secret key also contained in the user's SIM card. It is used for authentication and for ciphering on the radio channel.
- ***Gateway Mobile Switching Centre (GMSC):*** The GMSC is the point to which a ME terminating call is initially routed, without any knowledge of the MS's location. The GMSC is thus in charge of obtaining the MSRN (Mobile Station Roaming Number) from the HLR based on the MSISDN (Mobile Station ISDN number, the "directory number" of a MS) and routing the call to the correct visited MSC. The "MSC" part of the term GMSC is misleading, since the gateway operation does not require any linking to an MSC.
- ***SMS Gateway (SMS-G):*** The SMS-G or SMS gateway is the term that is used to collectively describe the two Short Message Services Gateways defined in the GSM standards. The two gateways handle messages directed in different directions. The SMS-GMSC (Short Message Service Gateway Mobile Switching Centre) is for short messages being sent to an ME. The SMS-IWMSC (Short Message Service Inter-Working Mobile Switching Centre) is used for short messages originated with a mobile on that network. The SMS-GMSC role is similar to that of the GMSC, whereas the SMS-IWMSC provides a fixed access point to the Short Message Service Centre.

Operation and Support Subsystem (OSS)

The OSS or operation support subsystem is an element within the overall GSM network architecture that is connected to components of the NSS and the BSC. It is used to control and monitor the overall GSM network and it is also used to control the traffic load of the BSS. It must be noted that as the number of BS increases with the scaling of the subscriber population some of the maintenance tasks are transferred to the BTS, allowing savings in the cost of ownership of the system.

3.2. Security issues in 2G wireless mobile networks

Main 2G/GSM security concerns are:

Man in the-middle attack:-This attacker positions itself between the target user and a network **eavesdropping** and modifying the traffic.

Eavesdropping:-The attacker eavesdrops Signalling and data connections.

Network Impersonation:- the attacker sends signalling and data to the target user pretending to be a genuine network.

User Impersonation:- the intruder sends signalling data to the network pretending to be originated by the target user.

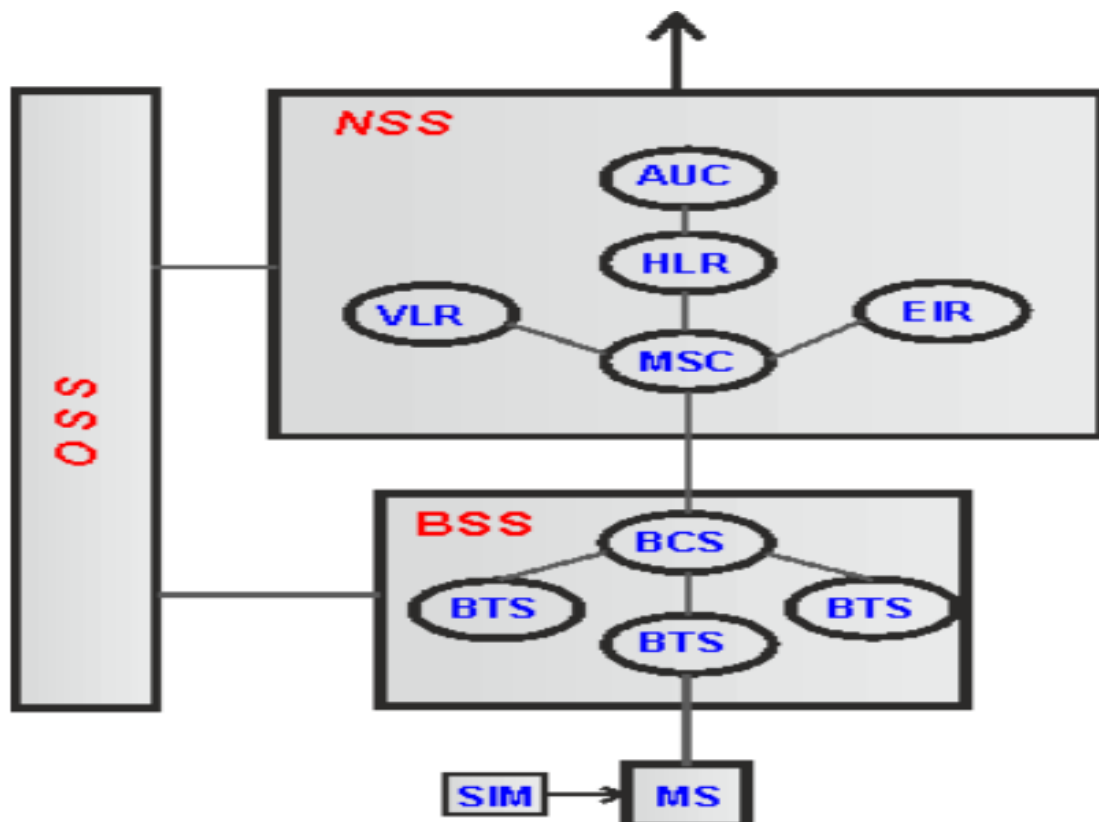


Figure 1 Simplified GSM Network Architecture Diagram.

The security enhancement using Encryption security feature:

Is encoding of a message or information in such a way that only authorized parties can access it. The raw data is encrypted using encryption algorithm (i.e. cipher). Then a data can be read only after decrypted by authorized receiver with the key generated. However no encrypted calls are still available in 2G due to imperfectly-designed encryption scheme. Also

Operator can control the use of the system by the provision of the Subscriber Identity Module (SIM) which contains a **user identity** and **authentication key**. This keeps to the minimum the level of trust the Operator needs to place in the user, serving network and manufacturer of the Mobile Equipment (ME). Use A5/1 stream cipher security protocol.

Also Operator can control the use of the system by the provision of the Subscriber Identity Module (SIM) which contains a **user identity** and **authentication key**. This keeps to the minimum the level of trust the Operator needs to place in the User, Serving Network and manufacturer of the Mobile Equipment (ME). Use A5/1 stream cipher security protocol.

CHAPTER 4

SECURITY IN THIRD GENERATION WIRELESS MOBILE TECHNOLOGY (3G)

4.1 Features of 3G

The primary reason for the development of the 3G system is to make **higher value services** available. 3G uses CDMA/CDD. It introduced the 2100MHz circuit switched network. Data rate of third generation wireless mobile network is 3.1 Mbps

4.2 Types of Threats for 3G

As the n of Users, Service Providers, and Network Operators in the market expands; Networks became smaller & more numerous. Thus, opportunity created for deliberate abuse or unintentional mishaps. Authentication and Key Agreement (AKA) protocol is at the core of 3G air interface security. It is used for mutual authentication and authenticated key establishment. This is regularly performed between the visited network and the mobile phone, the user equipment (UE).It involves the network sending authentication request to the UE. The UE checks the validity of this request (thereby authenticating the network), and then sends a user authentication response .The network checks this response to authenticate the UE. As a result, if successful, the two parties have authenticated each other, and at the same time they establish two shared secret keys. To participate in the protocol, the SIM inside UE must possess 2 things: A long term secret key K, known only to the users' SIM and to the SIM's 'home network' and a sequence number (SQN) maintained by both the USIM and the home network.

Unauthorised access to sensitive data (violation of confidentiality):-

Eavesdropping: An intruder intercepts messages without detection.

Masquerading: An intruder hoaxes an authorised user into believing that they are the legitimate system to obtain confidential information from the user; or an intruder hoaxes a legitimate system into believing that they are an authorised user to obtain system service or confidential information.

Traffic analysis: An intruder observes the time, rate, length, source, and destination of messages to determine a user's location or to learn whether an important business transaction is taking place. Browsing: An intruder searches data storage for sensitive information. - Leakage: An intruder obtains sensitive information by exploiting processes with legitimate access to the data.

Inference: An intruder observes a reaction from a system by sending a query or signal to the system. An intruder may actively initiate communications sessions and then obtain access to information through observation of the time, rate, length, sources or destinations of associated messages on the radio interface. Unauthorised manipulation of sensitive data (Violation of integrity).Manipulation of messages: Messages may be deliberately modified, inserted, replayed, or deleted by an intruder. Disturbing or misusing network services (leading to denial of service or reduced availability).

Intervention: An intruder may prevent an authorised user from using a service by jamming the user's traffic, signalling, or control data.

Resource exhaustion: An intruder may prevent an authorised user from using a service by overloading the service.

Misuse of privileges: A user or a serving network may exploit their privileges to obtain unauthorised services or information.

Abuse of services: An intruder may abuse some special service or facility to gain an advantage or to cause disruption to the network.

Repudiation: A user or a network denies actions that have taken place.

- Solutions to the threats:
- Using an event-based GTP IPS as a countermeasure to protect **this** key protocol suite.

4.3 Security enhancement in 3G wireless and mobile technology

WAP (Wireless access Protocols):

The Wireless Application Protocol (WAP) is a worldwide standard for the delivery and presentation of wireless information to mobile phones and other wireless devices. The idea behind WAP is simple: simplify the delivery of Internet content to wireless devices by delivering a comprehensive, Internet-based, wireless specification. The WAP Forum released the first version of WAP in 1998. Since then, it has been widely adopted by wireless phone manufacturers, wireless carriers, and application developers worldwide. Many industry analysts estimate that 90 % of mobile phones sold over the next few years will be WAP-enabled.

The driving force behind WAP is the WAP Forum component of the Open Mobile Alliance. The WAP Forum was founded in 1997 by Ericsson, Motorola, Nokia, and Open wave Systems (the latter known as Unwired Planet at the time) with the goal of making wireless Internet applications more mainstream by delivering a development specification and framework to accelerate the delivery of wireless applications. Since then, more than 300 corporations have joined the forum, making WAP the de facto standard for wireless Internet applications. In June 2002, the WAP Forum, the Location Interoperability Forum, SyncML Initiative, MMS Interoperability Group, and Wireless Village consolidated under the name Open Mobile Alliance to create a governing body that will be at the center of all mobile application standardization work.

The WAP architecture is composed of various protocols and an XML-based markup language called the Wireless Markup Language (WML), which is the successor to the Handheld Device Markup Language (HDML) as defined by Openwave Systems. WAP 2.x contains a new version of WML, commonly referred to as WML2; it is based on the eXtensible HyperText Markup Language (XHTML), signaling part of WAP's move toward using common Internet specifications such as HTTP and TCP/IP.

In the remainder of this section we will take a look at the WAP programming model and the various components that comprise the WAP architecture. Where it is applicable, we will supply information on both the WAP 1.x and 2.x specifications. (More information on the leading markup languages used in wireless Internet applications is provided in Chapter 13.)

WAP Programming Model

The WAP programming model is very similar to the Internet programming model. It typically uses the *pull* approach for requesting content, meaning the client makes the request for content from the server. However, WAP also supports the ability to *push* content from the server to the client using the Wireless Telephony Application Specification (WTA), which provides the ability to access telephony functions on the client device.

Content can be delivered to a wireless device using WAP in two ways: with or without a WAP gateway. Whether a gateway is used depends on the features required and the version of WAP being implemented. WAP 1.x requires the use of a WAP gateway as an intermediary between the client and the wireless application server, as depicted in Figure 11.6. This gateway is responsible for the following:

- Translating requests from the WAP protocol to the protocols used over the World Wide Web, such as HTTP and TCP/IP.
- Encoding and decoding regular Web content into compact formats that are more appropriate for wireless communication.
- Allowing use of standard HTTP-based Web servers for the generation and delivery of wireless content. This may involve transforming the content to make it appropriate for wireless consumption.
- Implementing push functionality using WTA.

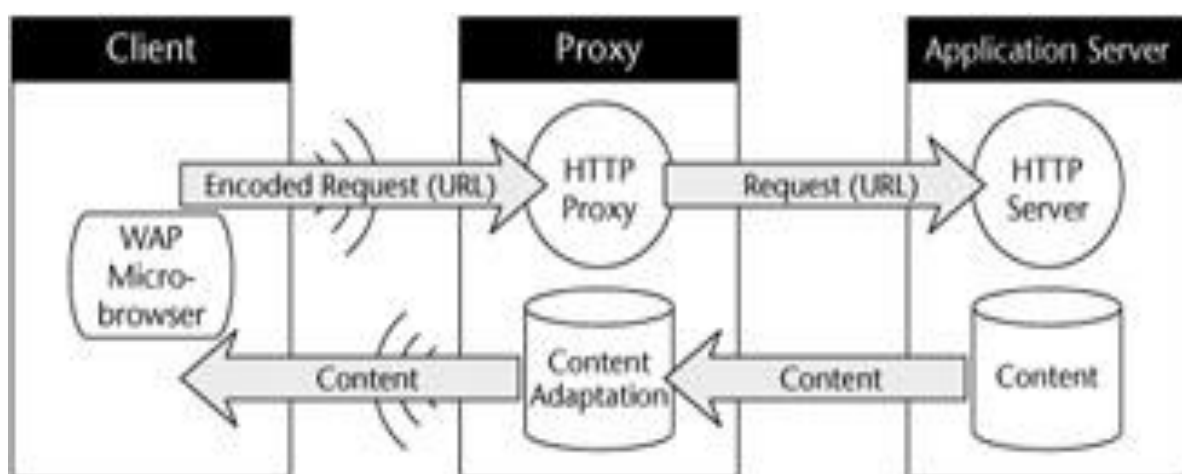


Figure 2 WAP Programming model using a wireless gateway (or proxy).

Note The WAP gateway is often called the *WAP proxy* in the WAP 2.x documents available from the OMA. In this chapter we continue to refer to it as the WAP gateway; just be

aware that both terms are used to refer to the same technology.

When developing WAP 2.x applications, you no longer are required to use a WAP gateway. WAP 2.x allows HTTP communication between the client and the origin server, so there is no need for conversion. This is not to say, however, that a WAP gateway is not beneficial. Using a WAP gateway will allow you to optimize the communication process and facilitate other wireless service features such as location, privacy, and WAP Push.

Figure 11.7 shows the WAP programming model without a WAP gateway: Note that removing it makes the wireless Internet application architecture nearly identical to that used for standard Web applications.

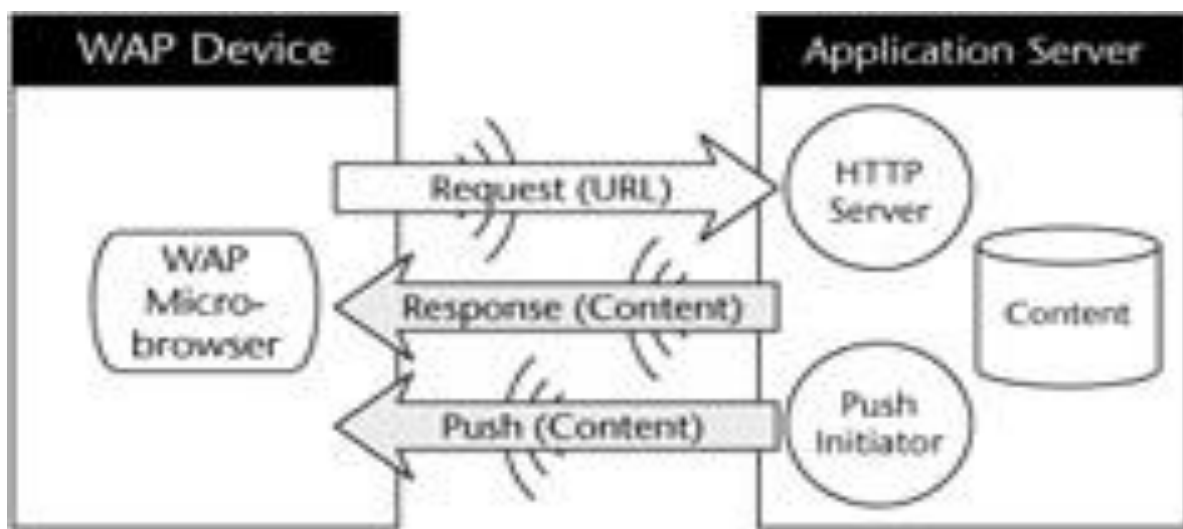


Figure 3: WAP programming model without gateway.

Both WAP programming models require the same core set of steps to process a wireless Internet request. These steps are based on the common pull model used for Internet applications; that is, a request/response method for communication. If you are interested in more details about how a wireless request is processed, refer back to the previous section of this chapter entitled *Processing a Wireless Request*.

WAP Components:-

The WAP architecture comprises several components, each serving a specific function. These components include a wireless application environment, session and transaction support, security, and data transfer. The exact protocols used depend on which version of WAP you are implementing. WAP 2.x is based mainly on common Internet protocols such as HTTP and TCP/IP, while WAP 1.x uses proprietary protocols developed as part of the WAP specification. We will investigate each component and its related function.

To begin, we will look at how WAP conforms to the Open Systems Interconnection (OSI) model as defined by the International Standards Organization (ISO). The OSI model consists of seven distinct layers, six of which are depicted in Figure 11.8 as they relate to the WAP

architecture. The physical layer is not shown; it sits below the network layer and defines the physical aspects such as the hardware and the raw bit-stream. For each of the other six layers, WAP has a corresponding layer, which will now be described in more depth.

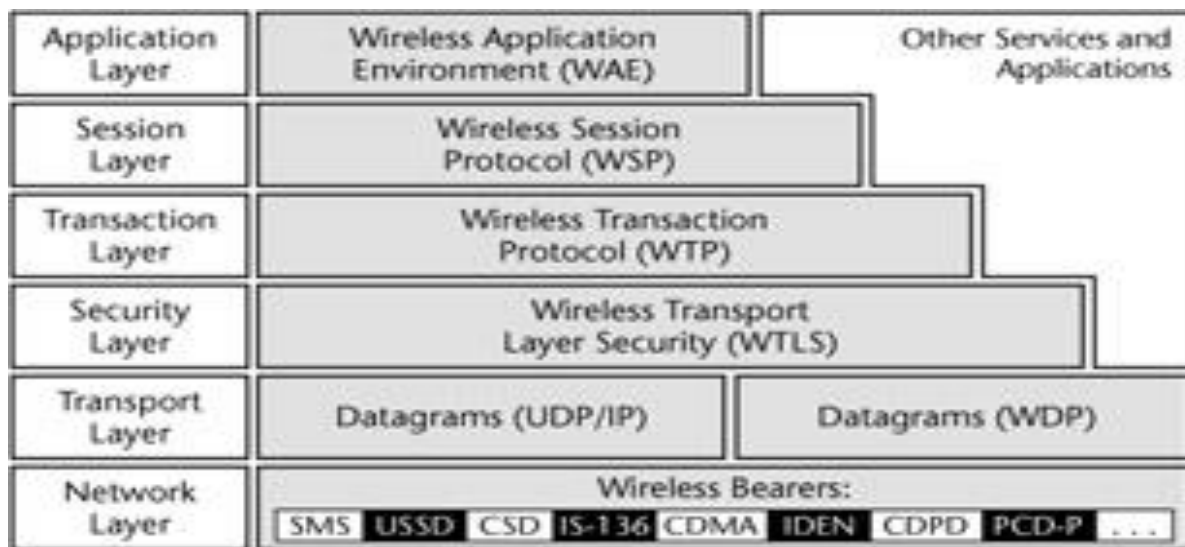


Figure 4: WAP architecture and its relationship to the OSI model.

Wireless Application Environment (WAE) :

The Wireless Application Environment (WAE) is the application layer of the OSI model. It provides the required elements for interaction between Web applications and wireless clients using a WAP microbrowser. These elements are as follows:

- A specification for a microbrowser that controls the user interface and interprets WML and WMLScript.
- The foundation for the microbrowser in the form of the Wireless Markup Language (WML). WML has been designed to accommodate the unique characteristics of wireless devices, by incorporating a user interface model that is suitable for small form-factor devices that do not have a QWERTY keyboard.
- A complete scripting language called WMLScript that extends the functionality of WML, enabling more capabilities on the client for business and presentation logic.
- Support for other content types such as wireless bitmap images (WBMP), vCard, and vCalendar.

WAP 2.x extends WAE by adding the following elements:

- A new markup language specification called WML2 that is based on XHTML-Basic. Backward compatibility with WML1 has been maintained.
- Support for stylesheets to enhance presentation capabilities. Stylesheet support is based on the Mobile Profile of Cascading Style Sheets (CSS) from the W3C, and supports both inline and external style sheets.

Note: WAP 2.x WAE has backward compatibility to WML1. This is accomplished either via built-in support for both languages or by translating WML1 into WML2 using eXtensible Stylesheet Language Transformation (XSLT). The method used depends on the implementation by the device manufacturer.

WAP Protocol Stack

The WAP protocol stack has undergone significant change from WAP 1.x to WAP 2.x. The basis for the change is the support for Internet Protocols (IPs) when IP connectivity is supported by the mobile device and network. As with other parts of WAP, the WAP 2.x protocol stack is backward-compatible. Support for the legacy WAP 1.x stack has been maintained for non-IP and low-bandwidth IP networks that can benefit from the optimizations in the WAP 1.x protocol stack.

We will take a look at both WAP 1.x and WAP 2.x, with a focus on the technologies used in each version of the specification.

WAP 1.x

The protocols in the WAP 1.x protocol stack have been optimized for low-bandwidth, high-latency networks, which are prevalent in pre-3G wireless networks. The protocols are as follows:

- **Wireless Session Protocol (WSP).** WSP provides capabilities similar to HTTP/1.1 while incorporating features designed for low-bandwidth, high-latency wireless networks such as long-lived sessions and session suspend/resume. This is particularly important, as it makes it possible to suspend a session while not in use, to free up network resources or preserve battery power. The communication from a WAP gateway to the micro-browser client is over WSP.
- **Wireless Transaction Protocol (WTP).** WTP provides a reliable transport mechanism for the WAP datagram service. It offers similar reliability as Transmission Control Protocol/Internet Protocol (TCP/IP), but it removes characteristics that make TCP/IP unsuitable for wireless communication, such as the extra handshakes and additional information for handling out-of-order packets. Since the communication is directly from a handset to a server, this information is not required. The result is that WTP requires less than half of the number of packets of a standard HTTP-TCP/IP request. In addition, using WTP means that a TCP stack is not required on the wireless device, reducing the processing power and memory required.
- **Wireless Transport Layer Security (WTLS).** WTLS is the wireless version of the Transport Security Layer (TLS), which was formerly known as Secure Sockets Layer (SSL). It provides privacy, data integrity, and authentication between the client and the wireless server. Using WTLS, WAP gateways can automatically provide wireless security for Web applications that use TLS. In addition, like the other wireless protocols, WTLS incorporates features designed for wireless networks, such as datagram support, optimized handshakes, and dynamic key refreshing.

- **Wireless Datagram Protocol (WDP).** WDP is a datagram service that brings a common interface to wireless transportation bearers. It can provide this consistent layer by using a set of adapters designed for specific features of these bearers. It supports CDPD, GSM, CDMA, TDMA, SMS, FLEX (a wireless technology developed by Motorola), and Integrated Digital Enhanced Network (iDEN) protocols.

WAP 2.x

One of the main new features in WAP 2.x is the use of Internet protocols in the WAP protocol stack. This change was precipitated by the rollout of 2.5G and 3G networks that provide IP support directly to wireless devices. To accommodate this change, WAP 2.x has the following new protocol layers:

- **Wireless Profiled HTTP (WP-HTTP).** WP-HTTP is a profile of HTTP designed for the wireless environment. It is fully interoperable with HTTP/1.1 and allows the usage of the HTTP request/response model for interaction between the wireless device and the wireless server.
- **Transport Layer Security (TLS).** WAP 2.0 includes a wireless profile of TLS, which allows secure transactions. The TLS profile includes cipher suites, certificate formats, signing algorithms, and the use of session resume, providing robust wireless security. There is also support for TLS tunneling, providing end-to-end security at the transport level. The support for TLS removes the WAP security gap that was present in WAP 1.x.
- **Wireless Profiled TCP (WP-TCP).** WP-TCP is fully interoperable with standard Internet-based TCP implementations, while being optimized for wireless environments. These optimizations result in lower overhead for the communication stream.

Note Wireless devices can support both the WAP 1.x and WAP 2.x protocol stacks. In this scenario, they would need to operate independently of each other, since WAP 2.x provides support for both stacks.

Other WAP 2.x Services:

In addition to a new protocol stack, WAP 2.x introduced many other new features and services. These new features expand the capabilities of wireless devices and allow developers to create more useful applications and services. The following is a summary of the features of interest:

- **WAP Push.** WAP Push enables enterprises to initiate the sending of information on the server using a push proxy. This capability was introduced in WAP 1.2, but has been enhanced in WAP 2.x. Applications that require updates based on external information are particularly suited for using WAP Push. Examples include various forms of messaging applications, stock updates, airline departure and arrival updates,

and traffic information. Before WAP Push was introduced, the wireless user was required to poll the server for updated information, wasting both time and bandwidth.

- **User Agent Profile (UAProf).** The UAProf enables a server to obtain information about the client making the request. In WAP 2.x, it is based on the Composite Capabilities/Preference Profiles (CC/PP) specification as defined by the W3C. It works by sending information in the request object, allowing wireless servers to adapt the information being sent according to the client device making the request.
- **External Functionality Interface (EFI).** This allows the WAP applications within the WAE to communicate with external applications, enabling other applications to extend the capabilities of WAP applications, similar to plug-ins for desktop browsers.
- **Wireless Telephony Application (WTA).** The WTA allows WAP applications to control various telephony applications, such as making calls, answering calls, putting calls on hold, or forwarding them. It allows WAP WTA-enabled cell phones to have integrated voice and data services.
- **Persistent storage interface.** WAP 2.x introduces a new storage service with a well-defined interface to store data locally on the device. The interface defines ways to organize, access, store, and retrieve data.
- **Data synchronization.** For data synchronization, WAP 2.x has adopted the SyncML solution. As outlined in Chapter 10, "Enterprise Integration through Synchronization," SyncML provides an XML-based protocol for synchronizing data over both WSP and HTTP.
- **Multimedia Messaging Service (MMS).** MMS is the framework for rich-content messaging. Going beyond what is possible for SMS, MMS can be used to transmit multimedia content such as pictures and videos. In addition, it can work with WAP Push and UAProf to send messages adapted specifically for the target client device.

WAP Benefits:

The WAP specification is continually changing to meet the growing demands of wireless applications. The majority of wireless carriers and handset manufacturers support WAP and continue to invest in the new capabilities it offers. Over the years WAP has evolved from using proprietary protocols in WAP 1.x to using standard Internet protocols in WAP 2.x, making it more approachable for Web developers. The following are some of the key benefits that WAP provides:

- WAP supports legacy WAP 1.x protocols that encode and optimize content for low-bandwidth, high-latency networks while communicating with the enterprise servers using HTTP.

- WAP supports wireless profiles of Internet protocols for interoperability with Internet applications. This allows WAP clients to communicate with enterprise servers, without requiring a WAP gateway.
- WAP allows end users to access a broad range of content over multiple wireless networks using a common user interface, the WAP browser. Because the WAP specification defines the markup language and microbrowser, users can be assured that wireless content will be suitable for their WAP-enabled device.
- WAP uses XML as the base language for both WML and WML2 (which uses XHTML), making it easy for application developers to learn and build wireless Internet applications. It also makes content transformation easier by incorporating support for XSL stylesheets to transform XML content. Once an application is developed using WML or WML2, any device that is WAP-compliant can access it.
- WAP has support for WTA. This allows applications to communicate with the device and network telephony functions. This permits the development of truly integrated voice and data applications.
- Using UAProf, the information delivered to each device can be highly customized. (Chapter 13 provides more details on how this information can be used to deliver user-specific content.)
- WAP works with all of the main wireless bearers, including CDPD, GSM, CDMA, TDMA, FLEX, and iDEN protocols. This interoperability allows developers to focus on creating their applications, without having to worry about the underlying network that will be used.

At present, all major wireless carriers support the WAP specification. This universal support is expected to continue as WAP evolves, providing a robust, intuitive way to extend Web content to wireless devices.

- Is an open specification which enables mobile users to access the Internet.
- It is independent of underlying network.

CHAPTER 5

SECURITY IN FOURTH GENERATION (4G) WIRELESS AND MOBILE TECHNOLOGY

5.1 Features of 4G

Represent a tech. of wireless Internet that hands you off to another network without interruption. So you may continue your activities online without even noticing that you connected into another network. Another name for it is "**seamless roaming**." It is developed by third generation partnership project (3GPP) at Norway in 2009. Offering any kind of services **anytime, anywhere**. The 4G network architecture is combination of multiple heterogeneous networks such as worldwide interoperability for microwave access (WiMAX) and 3G. Fourth generation operates on the IP protocol and architecture, just like Long term Evolution (LTE) and Wimax. It also uses Smart Antennas. Based on GSM/EDGE & UMTS/HSPA network technologies.

It is Faster and more reliable than 3G. Speed of data transmission is 100 Mb/s (802.11g wireless = 54Mb/s, 3G = 2Mb/s). Multi-standard wireless system. Bluetooth, Wired, Wireless (802.11x) Ad Hoc Networking. IPv6 Core Potentially IEEE standard 802.11n. Uses Orthogonal Frequency Division Modulation (OFDM) instead of CDMA. Using a large number of parallel narrow-band subcarriers instead of a single wide-band carrier to transport information. Very easy and efficient in dealing with multi-path. It is Robust against narrow-band interference. **Uses IPv6** which is of 128 bits. Mobile operators face unique risks due to the multitude of threat vectors involved; threats exist at the device, network, and application layers, and each must be considered and secured against to protect both the network and subscribers from attack.

5.2 Security Threats of 4G

4G mobile networks are all-IP, whereas 3G networks are a combination of IP and mobile signalling protocols (SS7). IP is much more open and well-known than the more obscure mobile protocols of the past, and has been successfully exploited by hackers for many years, opening up a number of potential threats. With 4G, encryption is only mandatory over the main Radio Access Network (RAN). The fact that 4G is an **open, heterogeneous** and **IP-based** environment, it will suffer from new security threats as well as inherent ones. Jamming UE Radio Interface: Jamming decreases the SNR by transmitting static and/or noise at P_{higher} levels across a given f_{band} . Research suggests that, due to the small amount of control signalling in LTE, this attack is possible.

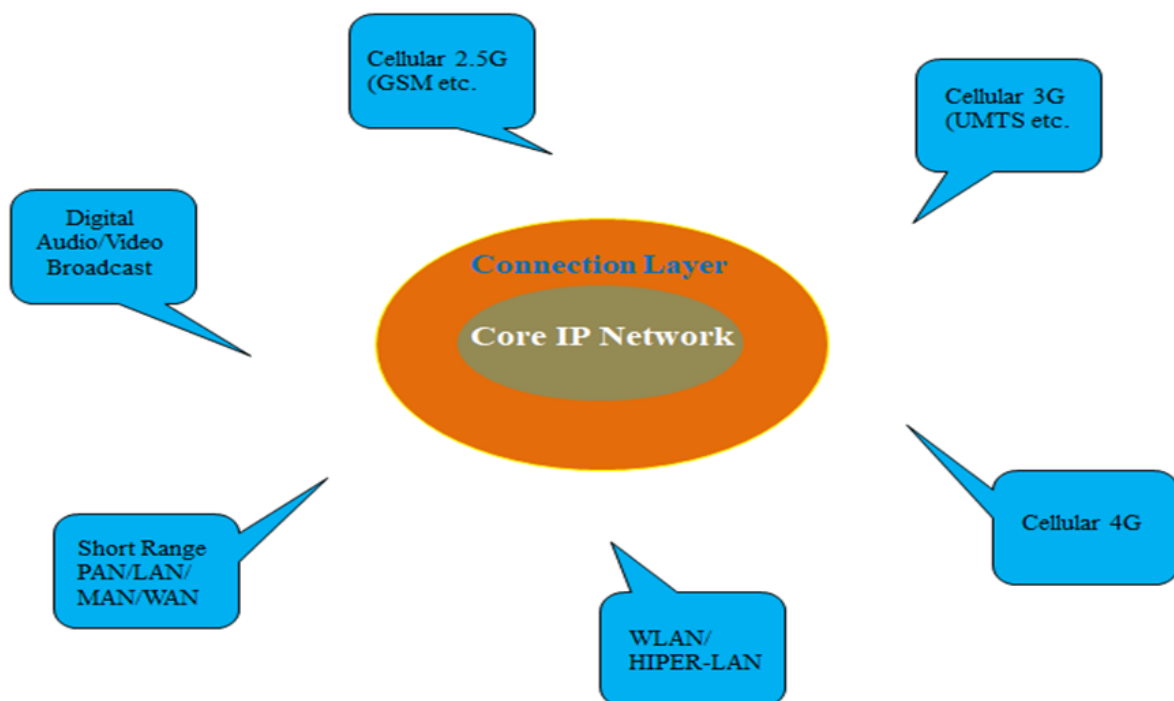


Figure 5 Seamless connections of networks in 4G

The eight Security dimensions analysis as depicted on figure 5.2

- Access control which measures protection level against unauthorized use of network resources.
- Authentication which measures confirmation level for the identities of each entity using the network.
- Non-repudiation which prove the origin of the data or identifies the cause of an event/action.
- Data confidentiality is to ensure that data is not disclosed to unauthorized users.

- e) Communication security is to allow information to flow only between authorized end points.
- f) Data integrity is to ensure the accuracy of data so that it can be modified, deleted, created or replicated without authorization and also provides an indication of unauthorized attempts to change the data.
- g) Availability is to ensure that there is no denial of authorized access to network elements, Store information, Information flows, services and applications due to network impacting events.
- h) Privacy is to provide for the protection of information that could be derived from the observation of network activities.

5.3. 4G Wireless and mobile technology Security Enhancement Issues

- a) Physical layer issues

Both WIMAX and LTE are subject to two key vulnerabilities at the physical layer. By deliberately inserting man-made interference on to a medium, a communication system can stop functioning due to a high signal-to-noise ratio. There are two types of interference that can be carried out: (i) noise (ii) multicarrier. Noise interference can be performed using white Gaussian noise (WGN). In the case of Multi-carrier interference, the attacker identifies carriers used by the system and injects a very narrowband signal on to those carriers. Interference attacks can be easily carried out as the equipment and knowledge to carry out such attacks are widely available.

Analysis indicates that interference is easy to detect using radio spectrum monitoring equipment's. Using radio-direction-finding tools, the interfering source can be traced. In addition, increasing the power of the source signal and using spreading techniques can increase its resilience against interference. While the possibility of interference is significant, since it is easy to detect and address, its believed that it's impact on the WIMAX/LTE network and users will be limited.

b) WiMAX-MAC-Layer security issues

To establish initial access with base station then IEEE802.16 [11] Radio interface standard describes several steps in order for a mobile station that includes seven steps. The steps are initial ranging and time synchronization, upper level parameter acquisition, basic capabilities negotiation, scanning and synchronization, mobile station authorization and key exchange, registration with the serving base station and the last step by which connection established. Among these steps five steps involved non secure traffic and two other two steps involved secure traffic exchange based on the device authentication standards of Wi-max.

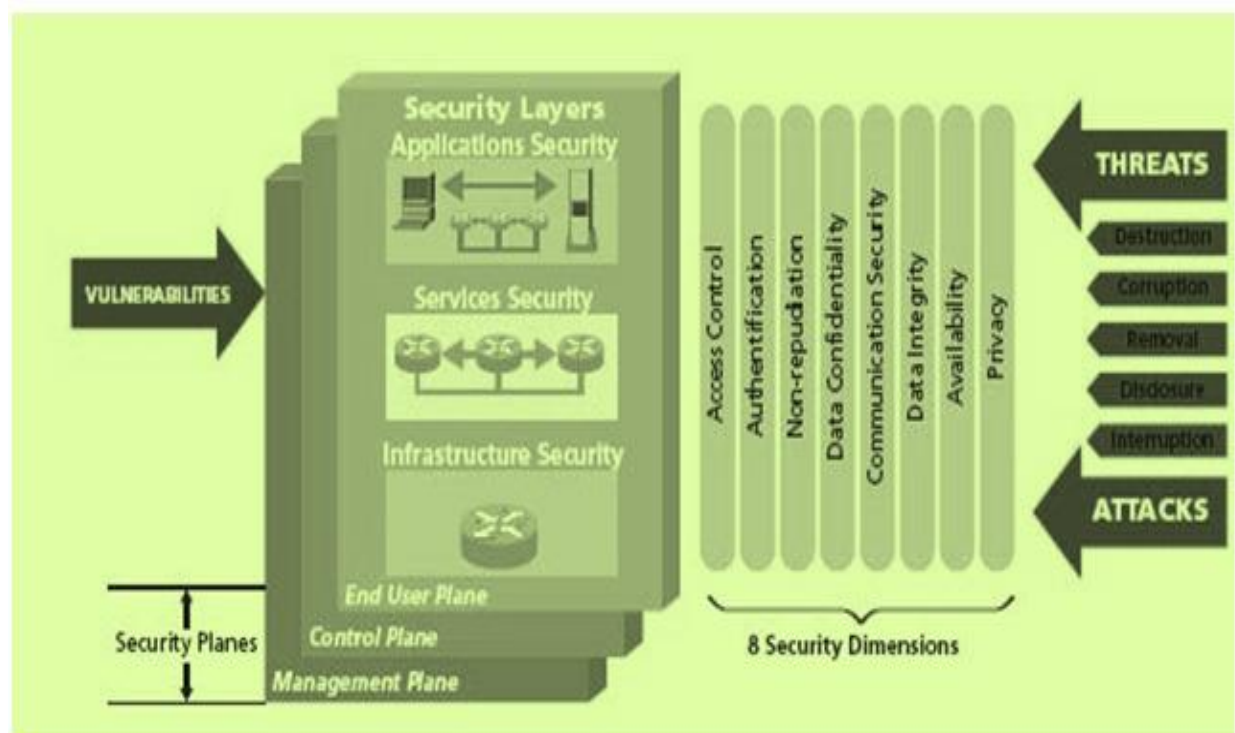


Figure 6 The eight Security dimensions of 4G

c) Denial of service security issues

The DoS attacks are a concern for Wi-max network. These attacks can be initiated through simple flooding attacking on authenticated management frames.

d)

Wireless LANs based on WI-FI technology have been available for more than a decade. However, the Wi-Fi technology has most often been used in homes and public places such as airports, hostels, and shopping malls where security is seeming less critical, although the cost benefits of Wi-Fi could be attractive to enterprise environments thanks to increased mobility, lower operational costs, and flexibility. Accordingly, security researchers have focused on security threats and solutions in Wi-Fi networks to make it applicable to the enterprise.

Environments. The original security mechanism of Wi-Fi called wired equivalent privacy (WEP), had a number of security flaws arising from the mis-application of cryptography, e.g. the use of RC4 stream cipher and CRC-32 authentication. Regarding this, a comprehensive security evaluation based on the ITU-T X.805 standard has been performed. To remedy the security flaws of Wi-Fi, several solutions have been proposed. The Robust Security Network (RSN) for the IEEE 802.1x standard's port based network access control is a layer-2 authentication mechanism and specifies how EAP can be encapsulated in the Ethernet frames. RSA Laboratory and Cisco have developed TKIP to mitigate the weakness of RC4 via frequent renewal of encryption key

CHAPTER 6

SECURITY IN FIFTH GENERATION (5G) WIRELESS AND MOBILE TECHNOLOGY

6.1 Features of 5G

It can be seen as a catalyst for minimizing the boundary between the digital world and physical world. Internets of Things (IoT) increase in variety of services. 5G systems are going to be service-oriented. For instance; a remote health care requires resilient security while IoT

requires lightweight security. This implies there will be a special emphasis on security and privacy requirements that stem from the angle of services. With the advances of mobile Internet, more and more vertical industries, including health care, smart home, and smart transport, will resort to 5G networks. Consumer mobile communications, video downloads and the use of mobile apps account for the bulk of 4G networks' radio resources usage today. With 5G, the goal will be to enable a much broader spectrum of uses and a much greater diversity of users. To target energy, healthcare, media, industry and transportation.

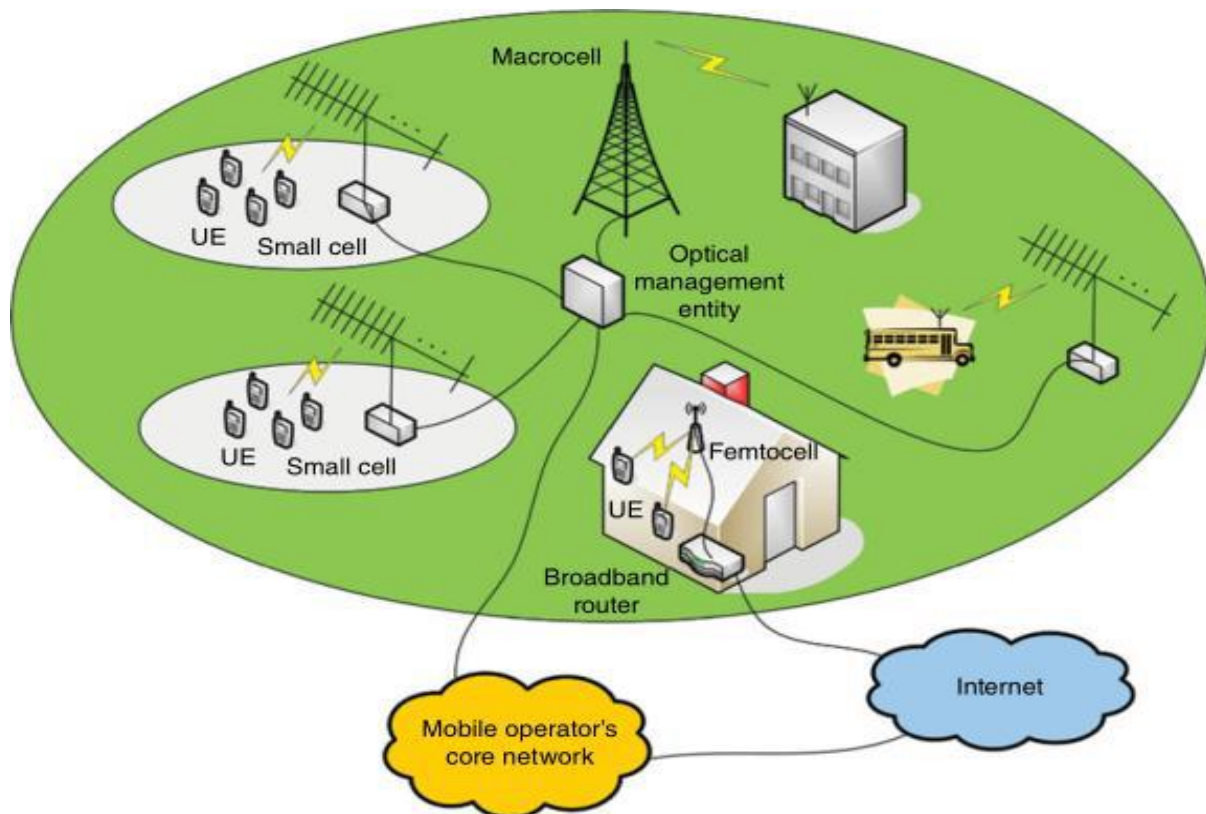


Figure 7 Architecture of proposed 5G technology

6.2 Security characteristics of 5G

So far, the drivers for mobile network evolution have mainly been about improving throughput and latency, and being able to better support the mobile internet. The drivers for security have remained in place to provide a trustworthy basic connectivity service. This basic trust will continue to be a driver for 5G networks as a high data-rate, mobile broadband service. However, additional key driving factors will enter the scene. First of all, 5G networks will be designed to serve not only new functions for people and society, but also to connect industries (such as manufacturing and processing, intelligent transport, smart grids and e-health). With 5G, it is possible to foresee new models of how network and communication services are provided. For example, a car manufacturer may wish to provide management services for cars. Establishing direct roaming agreements with various access network providers could be a cost-efficient way to achieve this. Similarly, the concept of terminal/ device will change: unattended machines and sensors will connect; sometimes entire capillary networks comprising tens or hundreds of individual devices will simultaneously attach to the 5G network. Next, new service delivery models will be used, involving new actors in the ecosystem. Cloud and virtualization technologies and anything-as-a-service will be used to reduce costs, and to deploy and optimize services more rapidly.

Telecom networks will expose application programming interfaces (APIs) toward users and third-party service providers to a higher degree, for example, for the purpose of optimized delivery using location awareness, content adaptation and caching. Such optimizations will sometimes be provided by third-party software executing on shared hardware platforms alongside dedicated telecom software. Furthermore, general awareness of user privacy in society has increased, leading to a greater focus on the protection of user metadata and communication. This issue becomes even more central with the developments in big data analytics. What characterizes 5G, even more than 4G, is that it will have a crucial role in the operation of society. The full scope of security, privacy and resilience will be a concern that spans far beyond technology. It will ultimately impact legal frameworks, regulation and actions by commercial entities and individuals. There will be increased regulatory involvement in how entire 5G systems will operate.

Implications for Security and Privacy: -

The drivers listed above can be grouped into four characteristics of 5G networks and their usage, each with implications for security and privacy. These characteristics are: new trust models, new service delivery models, an evolved threat landscape, and increased privacy concerns. So, how do these characteristics affect the way we need to approach security and privacy in 5G? Are there technological or other types of limitations in current 4G security? New trust models Trust models change over time. As a simple example, consider the bring-your-own-device trend in enterprises. Previously, all user devices could be assumed to be trustworthy, as they were all of the same type, all issued and

managed by the corporate IT department. Today, users want to use their personal devices instead, posing threats as potential Trojan horses behind corporate firewalls. For current mobile systems, the trust model is rather straightforward, involving a subscriber (and their terminal) and two operators (the home and serving networks).

Since 5G is aimed at supporting new business models and involves new actors, trust models will change, giving rise to extended requirements in areas such as authentication between various actors, accountability and non-repudiation. For example, for new critical services such as public safety, what security requirements will be projected onto the 5G networks? The new types of devices will span an extremely wide range of security requirements and will at the same time have very different security postures: industry automation control devices, shipping containers, vehicles forming entire capillary networks, tiny climate monitoring sensors and, next-generation tablets and smartphones. Devices have so far been assumed to comply with standards and not to deliberately attempt to attack networks. But how well protected are very low-cost devices? Can a single connected device be used as a stepping stone for cyber-attacks deep into the system? And what is the attack surface of a 5G system with billions of inexpensive, connected devices? The existing trust model obviously does not capture this evolved business and technological scenery of 5G. To ensure that 5G can support the needs of new business models, and ensure sufficient security, the trust model map must be redrawn. As such, this does not necessarily mean completely redesigning security. However, it is crucial to identify any significant shortcomings. This must begin by defining a new trust model.

Security for new service delivery models:

The use of clouds and virtualization emphasizes the dependency on secure software, and leads to other effects on security. Current 3GPP-defined systems are based on functional node specifications and abstract interfaces (reference points) between them, and as such provide a good starting point for virtualization. Until now, however, dedicated/proprietary hardware has still often been used for these nodes and interfaces. Decoupling software and hardware means that telecom software can no longer rely on the specific security attributes of a dedicated telecom hardware platform. For the same reason, standard interfaces to the computing/network platforms – such as those defined by ETSI (the European Telecommunications Standards Institute) in their Network Functions Virtualization work – are necessary to ensure a manageable approach to security. When operators host third-party applications in their telecom clouds, executing on the same hardware as native telecom services, there are increased demands on virtualization with strong isolation properties. Evolved threat landscape 5G networks will serve an even more central role as critical infrastructure. Many people will have already experienced occasions when fixed telephone lines, internet access and the TV service have all stopped working at the same time during a major network outage. And societies certainly do not want to lose electrical power, mobile telephony and more at the same time. Today's networks host various values – examples include revenue streams and brand reputation.

The accessibility of these values via the internet has already attracted activists, underground economies, cybercrime and cyber-terrorists. The values hosted in, and generated by, the 5G system are estimated to be even higher, and the assets (hardware, software, information and revenue streams) will be even more attractive for different types of attacks. Furthermore, considering the possible consequences of an attack, the damage may not be limited to a business or reputation; it could even have a severe impact on public safety. This leads to a need to strengthen certain security functional areas. Attack resistance needs to be a design consideration when defining new 5G protocols. Questionable authentication methods such as username/password need to be phased out.

More fundamentally, however, the new threats emphasize the need for measurable security assurance and compliance; in other words, verifying the presence, correctness and sufficiency of the security functions. Those using 5G will need answers to questions such as: is it safe to deploy a virtual machine on a given piece of hardware? And what security tests have been applied to the software? A key asset of the Networked Society will be data. The role that data currently plays in processes such as decision-making and value creation is changing. Being in control of personal data will be crucial for operational reasons, but this will also increase in importance in order to create competitive advantages. As the carriers of this data, 5G networks will need to provide adequate protection in the form of isolation and efficient transport of protected (encrypted/authenticated) data. The ubiquity of 5G devices and connectivity will not only affect the technological attack surface; the exposure to social engineering attacks will also increase. People claiming to be work colleagues or repair technicians, for instance, may contact an individual and request various kinds of access not only to the individual's information, but also to their devices.



Figure 8 The defining characteristics of 5G security

Increased privacy concerns there have been several recent news stories related to allegations of mass surveillance. Reports have also emerged of rogue base stations tracking users in major cities, and of extracting personal data without user knowledge. The protection of personal data has been discussed within the framework of the EU. It is being reviewed in standardization bodies such as the 3GPP and the IETF (Internet Engineering Task Force), and

debated in many other forums. A particularly sensitive asset is the user identifier(s). Ever since 2G, user privacy has been an important consideration. However, the benefits of full International Mobile Subscriber Identity (IMSI) protection have so far not seemed to outweigh the complexity of implementing it.

Standardization Approach

Accepting that 5G security needs are not mainly driven by increased bitrates and other quantitative aspects, there is also a need to avoid the temptation of addressing 5G security solutions as a quantitative issue. In the main, the level of 5G security is not defined by the number of security mechanisms specified. On the contrary, trying to address all possible requirements of every stakeholder in the same network could well lead to a reduced security level, or at least to a solution with security properties that are difficult to grasp. The first requirement is rather a well-designed, flexible security baseline, and assurance in the implementation of this baseline will be more important than the number of requirements as such.

A multi-stakeholder approach involving operators, vendors, regulators, policy-makers and representatives of 5G users (for example, industry segments) are fundamental to the security baseline of trustworthy, cost-efficient and manageable 5G networks. Pre-standardization consensus building, such as joint research by the different stakeholders, will be important. One example of such an initiative is the 5G for Sweden research program. This is a joint collaboration between academic institutions, telecom companies and other industries, with the purpose of taking a leading position in digitalization. Another example is 5G-ENSURE, which is cooperation between equipment vendors, operators, academic institutions and SMEs. This EU Horizon 2020 project will study the 5G security architecture and build basic enablers for 5G, such as network virtualization and identity management. A lack of such efforts can have a detrimental effect on time to market. For example, during the 4G LTE standardization phase, there was almost one year of discussions within the 3GPP before a decision could be made on whether to allocate radio interface protection in the eNodeB or in the core network. ETSI (3GPP) and the IETF will continue to be two important standardization bodies for 5G security, and defining a new trust model will be one of their first priorities. Depending on the role that 5G aspires to play in new usages – for example, for enterprises, public safety and industrial automation, standards defined (or to be defined) by bodies such as the ISO (International Organization for Standardization), the IEC (International Electro technical Commission) and the CSA (Cloud Security Alliance) will also have an impact on the technology. Open source has already started to play a role in the development of 3G and 4G networks, and its importance will likely continue to grow.

6.3 Core 5G Security Topics

i) Security assurance

As discussed, it is likely that 5G networks will play an even more central role as critical infrastructure than earlier generations, and that security assurance will enter the picture to a higher degree. This is not a completely new development. The 3GPP has already observed the need to extend security specifications from functional ones for interfaces to assurance specifications on the node/interface implementations, and has initiated work known as SECAM. However, in combination with cloud-based implementation (virtualization and on-demand service) there is a likely need to separate software assurance more concretely from platform assurance, and to allow on demand measurements of assurance as part of Service Level Agreements (SLAs) and orchestration. Regarding the role of 5G networks as critical infrastructure, a decision must be made on just how critical these should be, since increasing criticality comes with a price tag in terms of assurance. The standard assurance for IT products is Common Criteria (ISO 15408). If 5G is to become a general platform for the Networked Society vision, it seems clear that Common Criteria compliance could enter as an additional assurance requirement on top of SECAM. However, the impact may not stop there. Assume that in some use cases, vehicle/road safety would be dependent on 5G network security. What does this imply? Today, safety-related car systems need to follow very comprehensive standards, such as ISO 26262. This is a 10-part standard, where, for example, part six covers safety related to software. Similarly, the health care sector is governed by standards such as ISO 27799 and, in the US, the HIPAA (Health Insurance Portability and Accountability Act).

For smart grids, demonstrated compliance with standards from the IEEE (Institute of Electrical and Electronics Engineers), the IEC and the NIST (National Institute of Standards and Technology) may apply. If 5G security becomes a critical link in the control loop of all of these applications, would it imply that 5G networks need to be certified against (parts of) all these standards? Although there will most likely be many overlapping compliance requirements, it is clear that considerable costs will be incurred on 5G network products. Will these costs be prohibitive and prevent 5G from providing valuable services to these applications? The answer is no, and there are at least two ways to handle this security overload on the 5G network. First, the concept of network slicing could be an important tool to handle the very diverse requirements of different applications and user groups. Slicing is often seen as a way to provide isolated sub-networks, each optimized for specific types of traffic characteristics. One such characteristic could be related to security and safety requirements. By having a properly implemented, high-assurance isolation mechanism to support slicing, it will be possible to confine the impact of security requirements to single slices, rather than the whole network. The cost of high assurance and certification can therefore be concentrated onto an infrastructure virtualization/ isolation layer.

The general approach could be to define a limited number of standardized, interoperable, high-assurance security enablers that are present in all slices as a baseline. On top of this, more application-specific security mechanisms are enabled by boot-strapping into specific slices, providing the additional security functions. Indeed, with a properly operating

virtualization layer, external parties such as enterprises could securely deploy their own (certified) software inside the 5G network, thereby offering governance to organizations using 5G, and at the same time reducing the number of certifications that the 5G network must undergo. Secondly, we have the choice to “factor out” security requirements from the 5G network slices by simply putting the responsibility in the endpoints; in other words, in connected devices or organization data centres.

Data security is an example of a service that could be handled this way. In summary, the fact that 5G is designed to be a platform for a wide range of new user groups and applications does not automatically mean that it is necessary (or even desirable) for the 5G network to carry all security responsibility and related costs. On the other hand, 5G networks clearly can provide some highly valuable security services. Besides the isolation/slicing itself, many other examples of network-enabled security as a service will be attractive to multiple user groups, including network enforced security policies, authentication, key management and data security services.

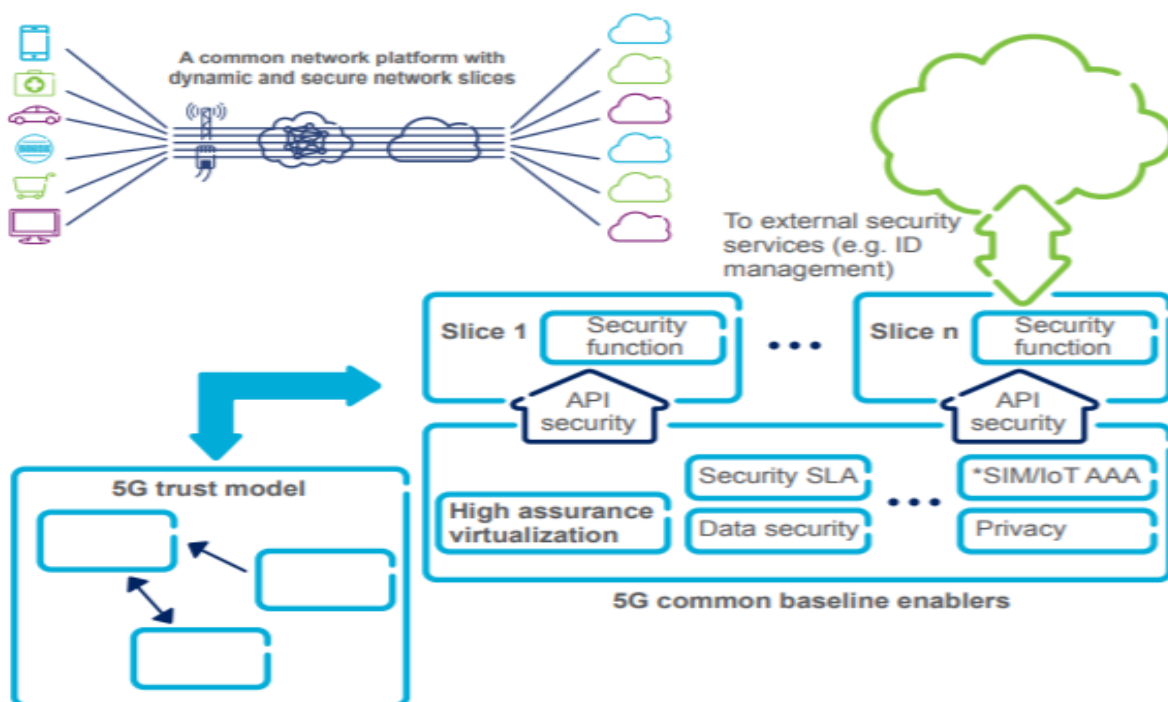


Figure 9 High level 5G security Principles

ii) Identity management

The 4G LTE standard requires USIM on physical Universal Integrated Circuit Cards to gain network access. This way of handling identity will continue to be an essential part of 5G for reasons such as the high level of security and user friendliness. Embedded SIM has also significantly lowered the bar for deployment issues related to machine-to-machine communication. Still, there is a general trend of bring-your-own-identity, and the 5G ecosystem would generally benefit from a more open identity management architecture that allows for alternatives. One example would be to allow an enterprise with an existing, secure ID management solution to reuse it for 5G access. Examining new ways to handle

device/subscriber identities is therefore a key consideration that should enter the investigation of the new trust models for 5G. Concepts such as network slicing can provide an enabler for securely allowing different ID management solutions side-by-side by confining usage to virtual, isolated slices of the network. The threat of IMSI catching, where rogue radio network equipment requests mobile devices to reveal their identity, was discussed during the 3G and 4G standardization process. However, no protection mechanism was introduced at that time, as the predictable threats did not seem to justify the cost or complexity involved. It is not clear whether this risk analysis is still valid, and enhanced IMSI protection deserves consideration for 5G.

iii) 5G radio network security

Due to the evolved threat landscape and new technology that provides users with low-cost alternatives to program their own devices (even at radio access level), the attack resistance of radio networks should be a more clearly outspoken design consideration in 5G, analysing threats such as Denial of Service from potentially misbehaving devices, and adding mitigation measures to radio protocol design. Although LTE radio access has excellent cryptographic protection against eavesdropping, there is no protection against modifying or injecting user plane traffic. With 5G radio access as a building block in, for example, industrial automation, the potential benefits of adding integrity protection seem worthy of investigation.

iv) Flexible and scalable security architecture

With virtualization and more dynamic configurations entering the picture for 5G, it seems logical to consider a more dynamic and flexible security architecture for it. Security for synchronous aspects like RAN signalling could be located close to the access with a higher degree of independence from asynchronous security aspects, such as those related to the user plane, than today. This would allow for more efficient security handling, and limit threats to sensitive user data at the same time. New security designs with higher flexibility could also better address unnecessary conflicts between usability and security. For example, new network APIs could allow the network to perform service chaining, such as traffic optimizations, while still allowing data to be encrypted end-to-end. Energy-efficient security while security services such as encryption come with a cost, the expense is no longer an issue for mobile phones and similar devices.

The energy cost of encrypting one bit is one or two orders of magnitude less than transmitting one bit. However, for the most constrained, battery dependent devices with a long target life time, there may be a need to consider even more lightweight solutions, as every micro joule consumed could be of importance. Cloud security Cloud security is already an extremely hot topic, and it will be added to the list of 5G concerns. Entire books have been written on this subject, so there follows just a brief list of priorities for cloud security in a 5G context, motivated by the discussions above.

v) Develop hypervisors and network virtualization with high assurance on isolation.

As mentioned, investments in this area could pay off, as this would greatly simplify the handling of diverse security requirements in the same infrastructure. Build useful ecosystems and architectures from existing trusted computing tools and concepts for remote attestation, for example. Provide more efficient solutions for cloud-friendly data encryption (homomorphic encryption, allowing operations on encrypted data). Develop easy-to-use, trusted management of cloud systems and the applications that run there. Some of these continue to represent essential academic research topics.

6.4 Security infrastructure of 5G

Diversified system level protection of IT-aware infrastructure after IT technologies (e.g. Network functions virtualization_NFV & Software defined networking_SDN) are put into use, a vast array of system-level protections is in place to defend against distributed denial of service (DDoS) and other active attacks that may increase. New trust model and identity management. Telecom networks are responsible for authenticating user for network access only.

But, in 5G networks, a trust model with an additional element, the vertical service provider, is favoured possible design. Networks may cooperate with service providers to carry out an even secure and more efficient identity management.

- **The most attractive target in 5G will be:**
- User equipment.
- Access networks.
- Mobile core and
- external IP networks

The specialised networks may provide network services cater for the specialised end users such as medical agency running a network to provide medical services for her customers. Today traditional network provides hop by hop security by provide secure communication path between the communicating parties which may not be efficient in 5G environment which requires end to end security to serve these new forms of specialised networks. These new specialised networks will result in new trust model for 5G networks with an additional element of services compared to traditional 4G trust model as shown below

For the services and users, building an E2E data security chain could be a way to reduce the reliance on individual link security and simplifies security management.

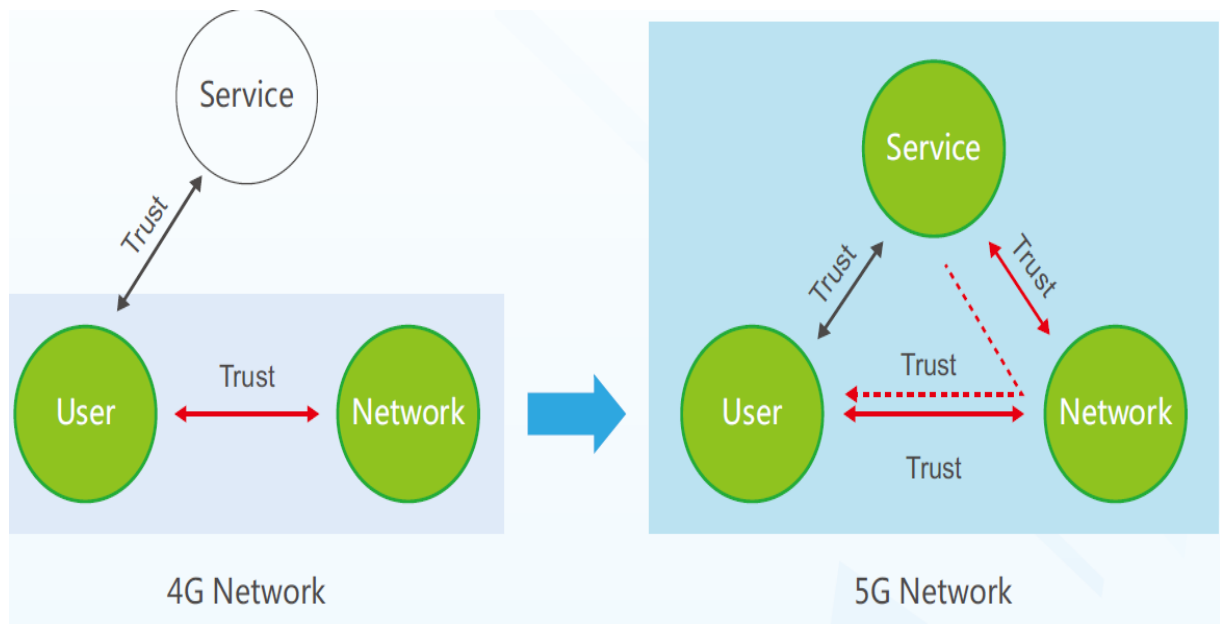


Figure 10 Link security level between user, network and service giver.

The Next Generation Mobile Network (NGMN) alliance highlights the following security requirements in 5G Whitepaper:

- Strong Subscriber Authentication
- Must provide the security mechanism for protecting diverse range of information.
- Bearer-independent (e.g., higher layer) security (end to end security)
- Secure network design
- Resilience and High Availability to provide 99.999% network availability
- Reliability

CHAPTER 7

CONCLUSION

Wireless and mobile networks have undergone a tremendous evolution since their start. This was mainly motivated by the need for connectivity everywhere, as exemplified by the philosophy of “always on” access. Mobile telephony was the first need felt by users, followed by the need for mobile Internet applications. Mobile telecommunications networks were the first concretization of mobile telephony, followed by a set of wireless technologies with or without embedded mobility and with or without infrastructure. Obviously, this large deployment of services over mobile and wireless networks is not easy from a network security point of view. This Seminar presented selected up-to-date investigation on security in five generations of wireless and mobile environments. The security dimension of the upcoming or proposed 5G technology is anticipated; and the additional feature it is intended to offer is clearly observed.

REFERENCES

[1] Boyle and Panko, Corporate Computer Security, 3/e (2013, Prentice Hall). See also: Panko, Corporate Computer and Network Security, 2/e (2009, Prentice Hall).

[2] 4G LTE Cellular Technology: Network Architecture and Mobile Standards. [online].

Available: https://www.ermt.net/docs/papers/Volume_5/12_December2016/V5N12-118.pdf

[3] Another Look at Privacy Threats in 3G Mobile Telephony.[online].

Available: <https://pure.royalholloway.ac.uk/portal/files/19681499/alapti.pdf>

[4] Just HOW SECURE IS 4G ? [online].

Available: <https://opengear.com/articles/just-how-secure-4g>

[5] Universal Mobile Telecommunications System (UMTS); 3G Security; Security Threats and Requirements (3G TS 21.133 version 3.1.0 Release 1999). [online]

Available:http://www.etsi.org/deliver/etsi_ts/121100_121199/121133/03.01.00_60/ts_121133_v030100p.pdf

[6] Anderson, Security Engineering: A Guide to Building Dependable Distributed Systems, 2/e (Wiley, 2008). The first edition (2001)

[7] Network Security: Private Communication in a Public World, C. Kaufman, R. Perlman and M. Speciner, Prentice-Hall, 1995

[8] Network Security Essentials, William Stallings, Prentice-Hall, 2000

